Cisco

650-153

ESFE Cisco Email Security Field Engineer(R) Specialist

QUESTION: 90
When a message is matched on by a DLP policy, and the message is classified as 'Critical", what is the default remediation?

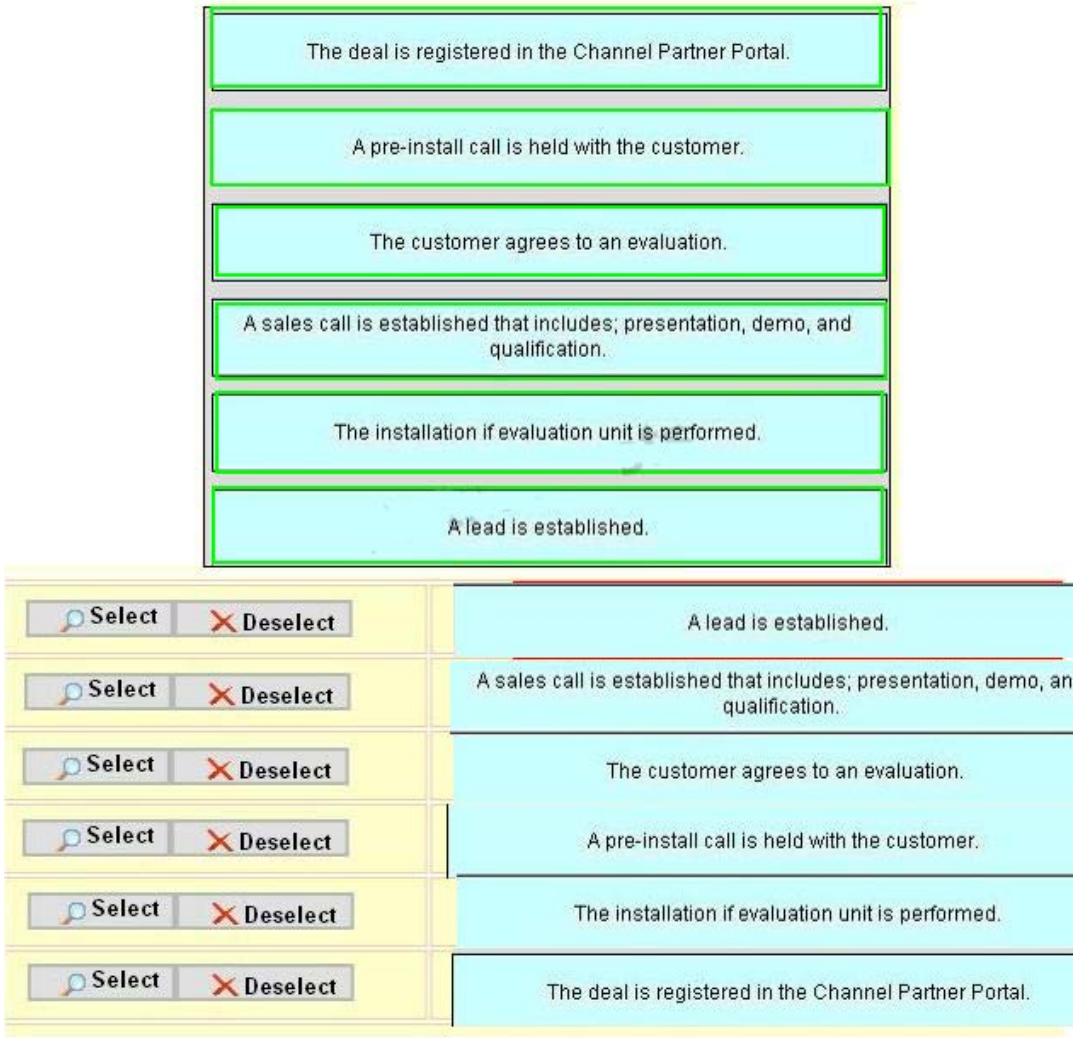
A. Deliver
B. Drop
C. Quarantine
D. Encrypt

Answer: B

QUESTION: 91
DRAG DROP
Place the following steps of the Evaluation Life Cycle in the correct order.

Select Deselect		Step 1
Select Deselect		Step 2
Select Deselect		Step 3
Select Deselect		Step 4
Select Deselect		Step 5
Select Deselect		Step 6

Answer:



QUESTION: 92
A customer using marketing message detection is reporting false positives. How should you advise them?

A. Turn off this feature and report the issue to customer support for fine tuning of the filter.
B. In the Anti-Spam configuration menu raise the marketing mail threshold. Using incoming mail reports to verify fewer false positives.
C. Send false positive samples to ham@access.ironport.com.
D. Send false positive samples to adds@access.ironport.com.

Answer: B

QUESTION: 93
Which of the following is the default Anti-Virus setting?

A.
Message scanning: Scan for Viruses only. Encrypted Attachments: Deliver, Unscannable Attachments: Deliver, Virus Infected Messages: Drop
B.
Message scanning: Scan and Repair, Encrypted Attachments: Deliver, Unscannable Attachments: Deliver, Virus Infected Messages: Drop
C.
Message scanning: Scan for Viruses only. Encrypted Attachments: quarantine, Unscannable Attachments: drop. Virus Infected Messages: Drop
D.
Message scanning: Scan for Viruses only. Encrypted Attachments: Deliver, Unscannable Attachments: Deliver, Virus Infected Messages: Deliver as an RFC 822 compliant attachment.

Answer: B

Explanation:
By default, these settings are enabled for the default Incoming Mail Policy:
anti-virus scanning results

Reference:
http://www.cisco.com/en/US/docs/security/esa/esa7.1/config_guide/ESA_7.1.1_Configuration_Gui de.pdf

QUESTION: 94
Using the customer requirements select the appropriate licenses keys that are needed. Customer wants to implement CRES on their outgoing mail. Incoming mail is handled by a hosted service. (Choose two.)

A. Bounce Verification
B. IronPort Email Encryption
C. IronPort Anti-Spam
D. Incoming Mail Handling / Receiving
E. Outbreak Filters
F. Sophos Anti-Virus

Answer: B, D

QUESTION: 95
Your customer has the default spam settings on their appliance. They need an immediate reduction in missed spam, but without increasing their false positive rate. How should you advise them?

A. In the HAT settings, increase the SBRS threshold for the BLACKLIST sender group.
B. Advise their end users to use the spam plugin or send false negatives samples to ham@access.ironport.com.
C. Enable Marketing Mail Detection.
D. Enable Intelligent Multi-Scan

Answer: D

Explanation:
IronPort Intelligent Multi-Scan incorporates multiple anti-spam scanning engines, including IronPort Anti-Spam, to provide an intelligent, multi-layer anti-spam solution. This method provides more accurate verdicts that increase the amount of spam that is caught but without increasing the false positives rate.

Reference:
http://www.cisco.com/en/US/docs/security/esa/esa7.1/config_guide/ESA_7.1.1_Configuration_Gui de.pdf

QUESTION: 96
Which of the following are best practice techniques when deploying content filters? (Choose Two)

A. Use the trace tool whenever possible.
B. Apply the filter in a test mail policy that contains one mailbox sender or recipient.
C. Run the 'filter test menue' before applying it to any mail policy.
D. Add an action to bcc all matches to your admin account.

Answer: B, C

QUESTION: 97
Which of the following security features are enabled for incoming mail by default? (Choose three)

A. bounce verification
B. IronPort Anti-Spam
C. Sophos Anti-Virus
D. McAfee Anti-Virus
E. Outbreak filters.

Answer: B, C, E

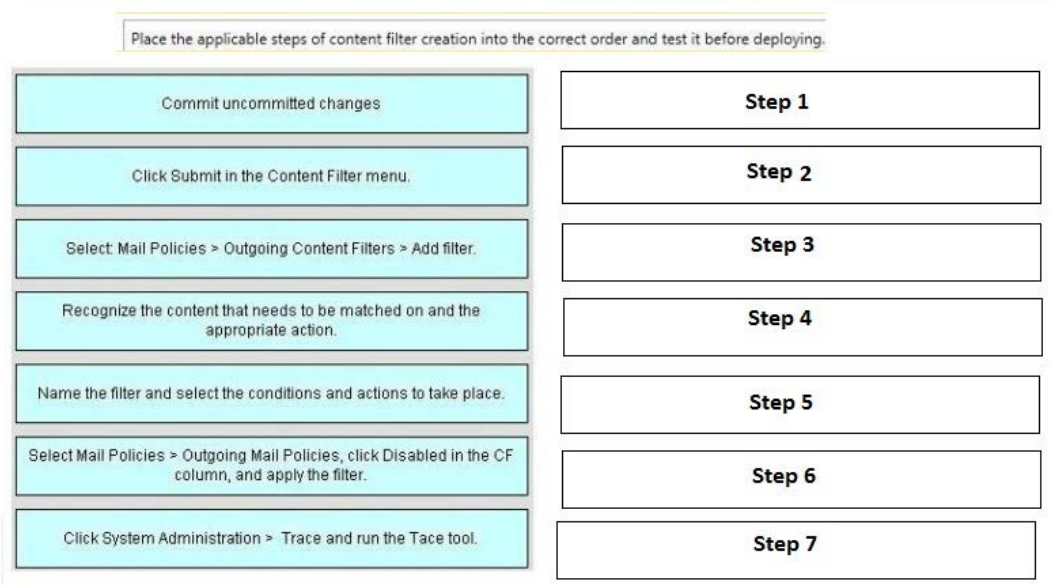
QUESTION: 98

Of the following which one is enabled by default on the C-Series?

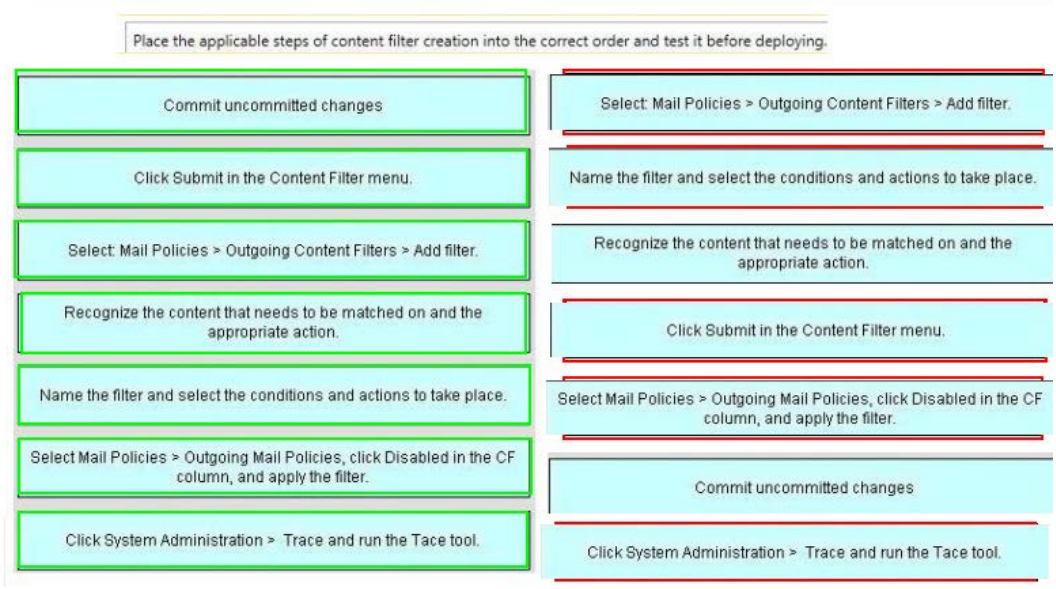
A. Local Reporting
B. Local Message tracking
C. Encryption
D. Bounce Verification

Answer: D

QUESTION: 99
DRAG DROP



Answer:



Explanation:

Step 1 - Select Mail Policies -- Outgoing Content filters -- Add filterStep 2 - Name the filter and select the conditions.....Step 3 - Recognize the content that needs to be matched...Step 4 - Submit in the Content Filter menuStep 5 - Select mail policies -- Outgoing Mail policies...Step 6 - Commit the changes Step 7 - Click System Administration -- Trace and run the trace tool